CUCM 버전 12.x에서 OS 관리자 및 DRS에 대한 SSO 구성

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager) 버전 12.0 이상에서 도입된 OS(운영 체제) 관리 및 DRS(재해 복구 시스템) 기능에 대한 SSO(단일 로그인)에 대해 설명합니다.

12.0 이전 버전의 CUCM은 CM Administration(CM 관리), Serviceability(서비스 가용성) 및 Reporting(보고) 페이지에만 SSO를 지원합니다. 이 기능은 관리자가 여러 구성 요소를 빠르게 탐색하고 더 나은 사용자 환경을 제공하는 데 도움이 됩니다. OS 관리자 및 DRS에 대해 SSO 중단이 발생하는 경우에도 복구 URL을 사용할 수 있는 옵션이 있습니다.

사전 요구 사항

요구 사항

CUCM 버전 12.0 이상에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 CCM(Cisco Call Manager) 버전 12.0.1.21900-7을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

OS Admin 및 DRS에 대해 SSO를 활성화하려면 CM Administration 로그인에 대해 SSO가 이미 활성화되어 있어야 합니다. 이 외에도, 새로운 사용자 또는 기존 사용자가 될 수 있는 플랫폼 레벨 사용자가 필요합니다.

기존 OS 관리자 사용자 사용

설치 시 생성된 플랫폼 사용자는 OS Admin 및 DRS 구성 요소의 SSO 로그인에 대해 구성할 수 있습니다. 이 경우 유일한 요구 사항은 이 플랫폼 사용자가 IdP(ID 제공자)가 인증된 AD(Active Directory)에도 추가되어야 한다는 것입니다.

새 사용자 사용

SSO OS 관리 및 DRS 로그인에 대해 새 사용자를 활성화하려면 다음 단계를 완료합니다.

1단계. Publisher의 CLI 액세스에서 권한 레벨 1/0의 새 사용자를 생성합니다.

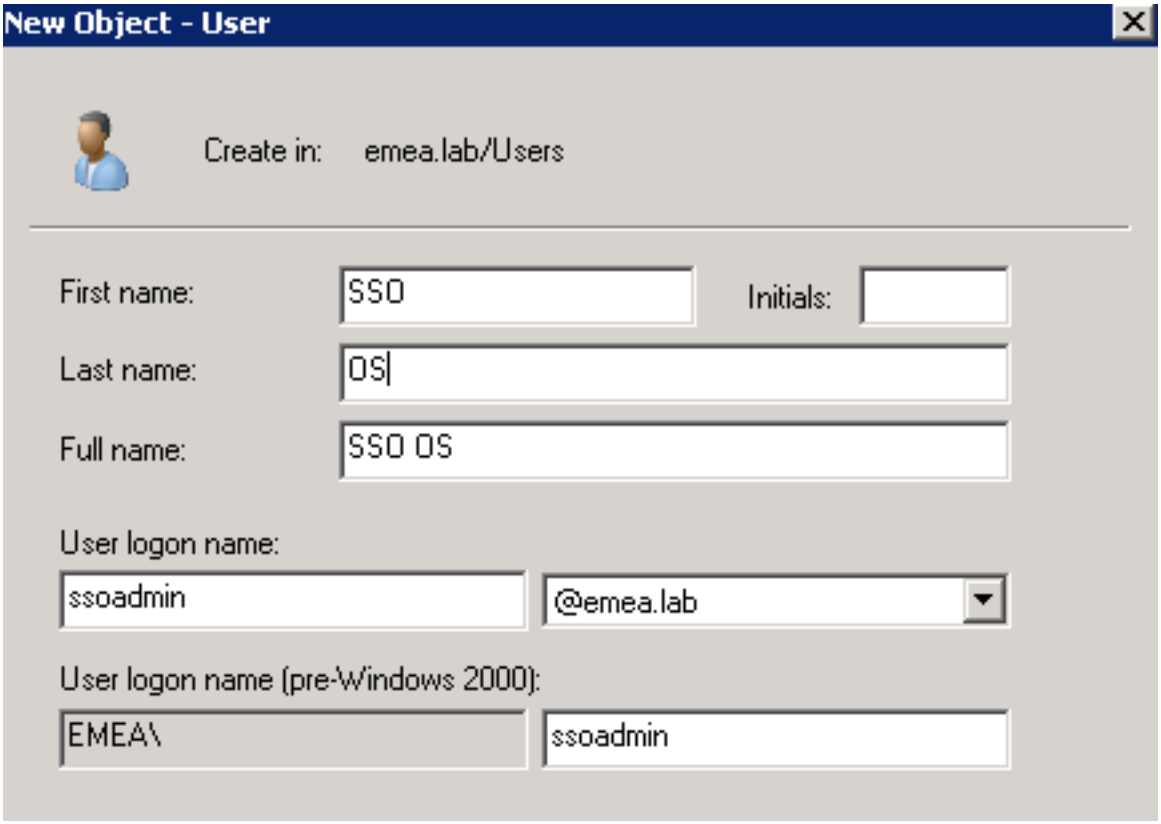
새로운 사용자를 만들기 위해서는 설치 시 생성한 플랫폼 사용자가 보유한 플랫폼 4 레벨 접속 권한이 필요합니다.

레벨 0 권한은 사용자에게 읽기 권한만 부여하며 레벨 1은 읽기 권한과 쓰기 권한을 모두 부여합니다.

```
admin:set account name ssoadmin



Privilege Levels are:

   Ordinary - Level 0

   Advanced - Level 1



Please enter the privilege level :1

Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No) :yes

To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that
identifies this user to LDAP (such as sAMAccountName or UPN).

        Please enter the appropriate LDAP Unique Identifier (UID) for this user:[ssoadmin]

Storing the default SSO UID value as username

Please enter the password :********

            re-enter to confirm :********

Account successfully created
```

여기에서 사용된 UID(Unique Identifier)에는 IdP가 어설션 응답에서 제공하는 값을 지정하거나 비워 둘 수 있습니다. 공백인 경우 CUCM은 사용자 ID를 **UID**로 사용합니다.

2단계. 그림과 같이 IdP가 인증되는 AD 서버의 이전 사용자 ID와 동일한 사용자 ID를 가진 사용자를 추가합니다.



3단계. 새로 생성된 사용자가 이미지에 표시된 대로 CUCM에 입력되도록 LDAP(Lightweight Directory Access Protocol) 서버의 동기화도 필요합니다.

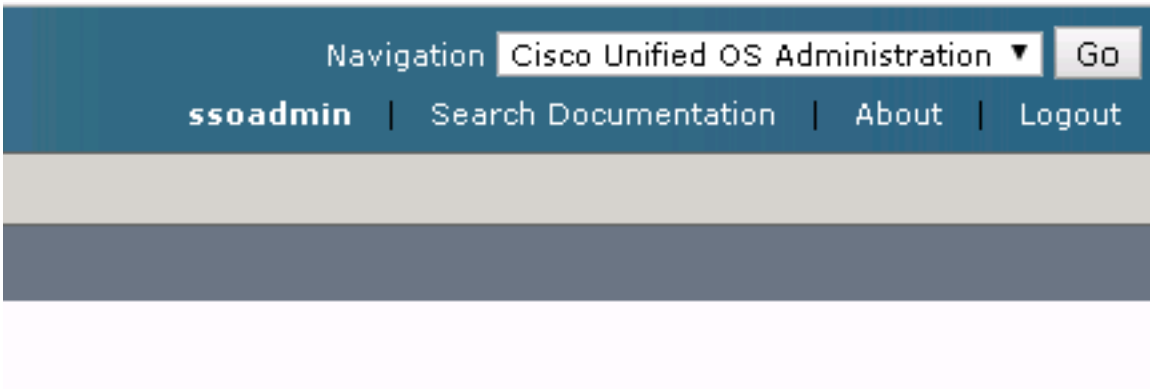
4단계. AD에 추가한 후 생성된 사용자에게는 (CLI를 통해) 비밀번호 재설정이 필요합니다.

```
login as: ssoadmin

ssoadmin@10.106.96.92's password:

WARNING: Your password has expired.

You must change your password now and login again!

Changing password for user ssoadmin.

Changing password for ssoadmin.

(current) UNIX password:

New password:

Re-enter password:
```

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

SSO가 OS Admin 및 DRS에 대해 성공적으로 활성화되면 로그인은 그림과 같이 이전에 생성한 사용자에 대한 AD의 크리덴셜을 사용하여 작동해야 합니다.



문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.